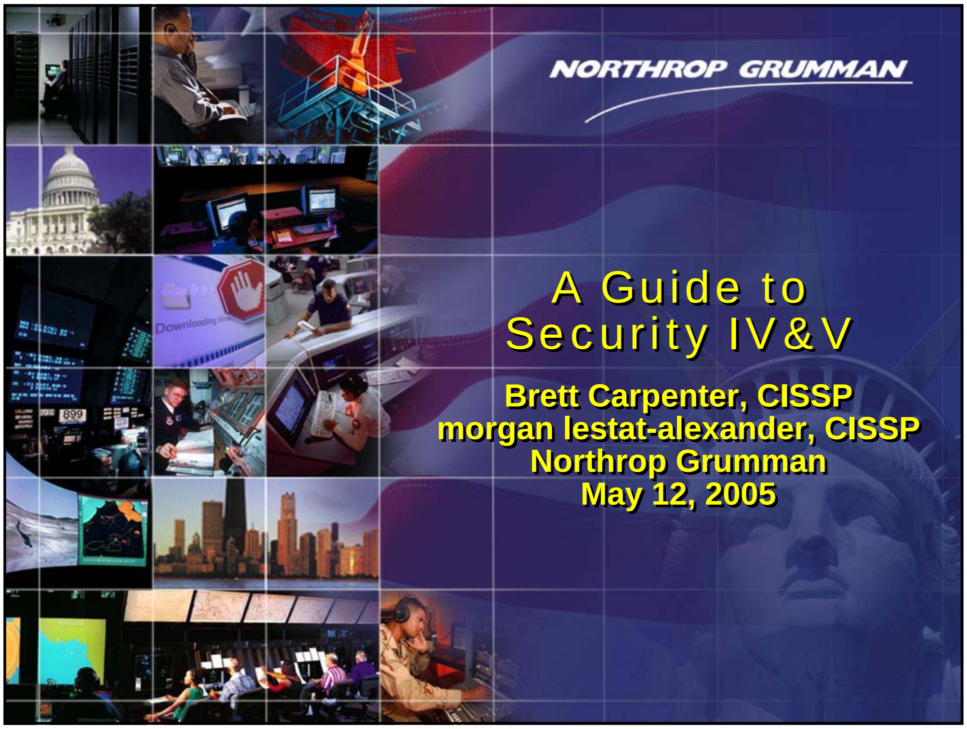
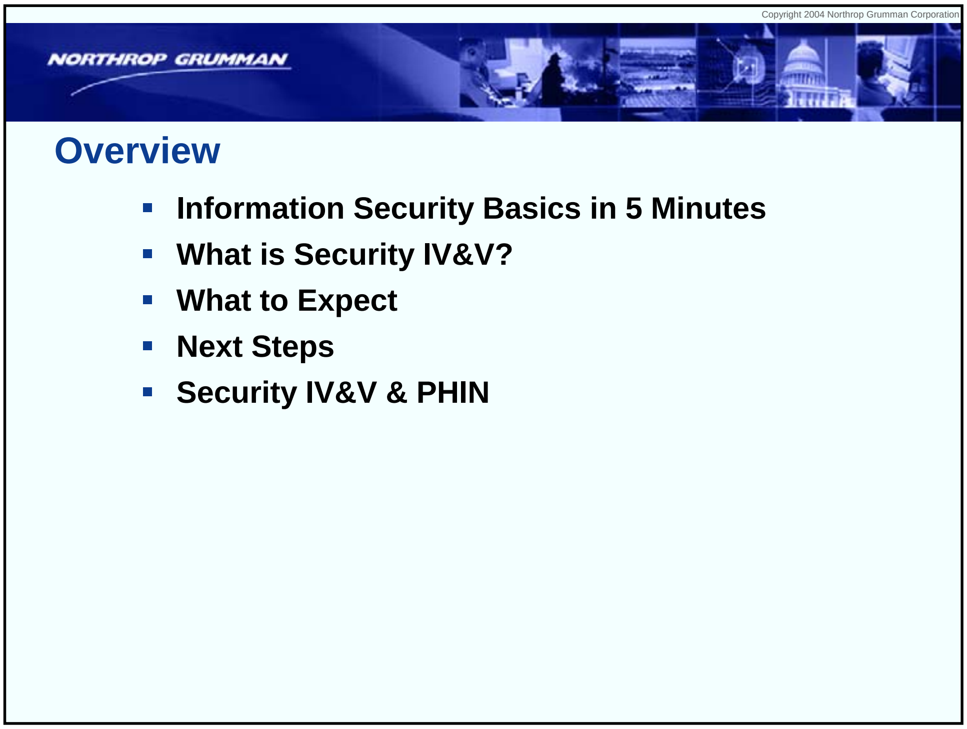


A Guide to Security IV&V

Brett Carpenter, CISSP
morgan lestat-alexander, CISSP
Northrop Grumman

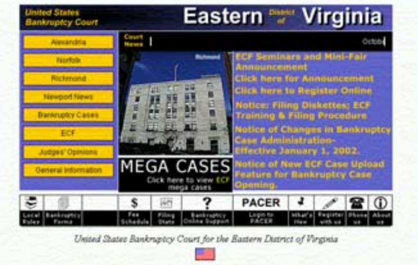
May 12, 2005



Overview

- Information Security Basics in 5 Minutes
- What is Security IV&V?
- What to Expect
- Next Steps
- Security IV&V & PHIN

First, A Peak At The Dark Side



ECF Seminars and Mini-Fair Announcement

Click here for Announcement

Click here to Register Online

Notice: Filing Diskettes; ECF Training & Filing Procedure

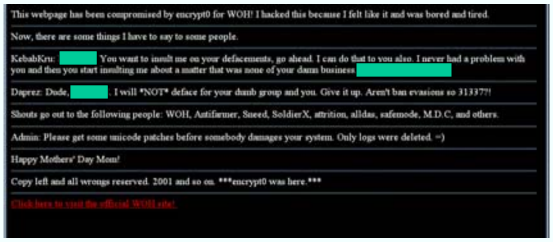
Notice of Changes in Bankruptcy Case Administration- Effective January 1, 2002.

Notice of New ECF Case Upload Feature for Bankruptcy Case Opening.

United States Bankruptcy Court for the Eastern District of Virginia

Before

After



This webpage has been compromised by encrypt0 for WOH! I hacked this because I felt like it and was bored and tired.

Now, there are some things I have to say to some people.

KebabKru: [redacted] You want to insult me on your defacements, go ahead. I can do that to you also. I never had a problem with you and then you start insulting me about a matter that was none of your damn business [redacted]

Daprez: Dude, [redacted]. I will *NOT* deface for your dumb group and you. Give it up. Aren't ban evasions so 31337?!

Shouts go out to the following people: WOH, Antifarmer, Sneed, SoldierX, attrition, alldas, safemode, M.D.C, and others.

Admin: Please get some unicode patches before somebody damages your system. Only logs were deleted. =)

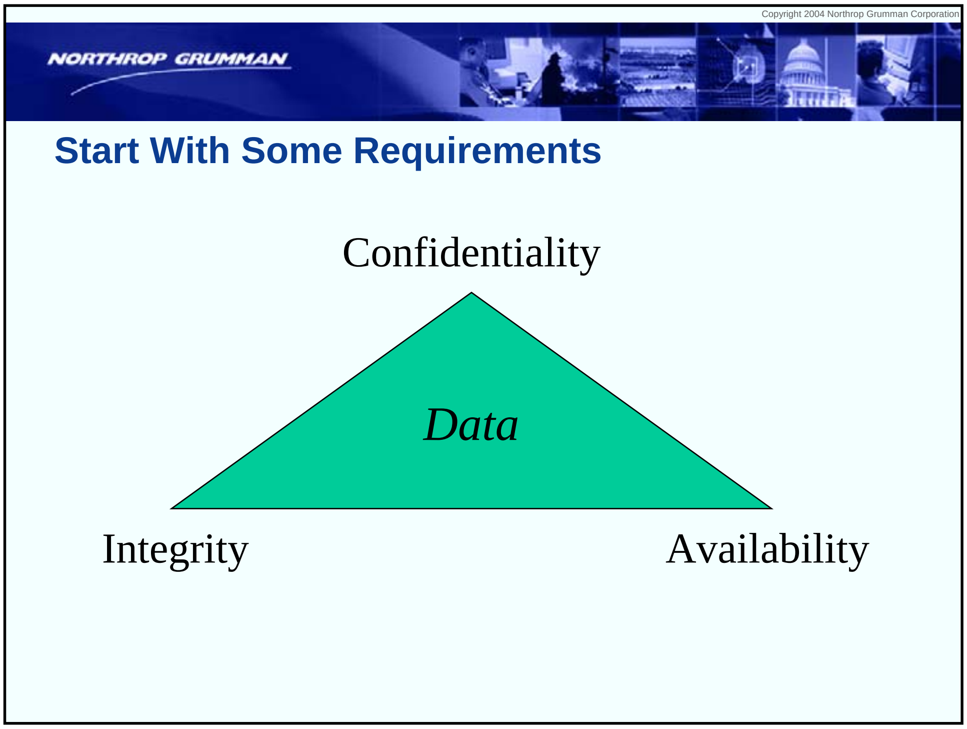
Happy Mothers' Day Mom!

Copy left and all wrongs reserved. 2001 and so on. ***encrypt0 was here.***

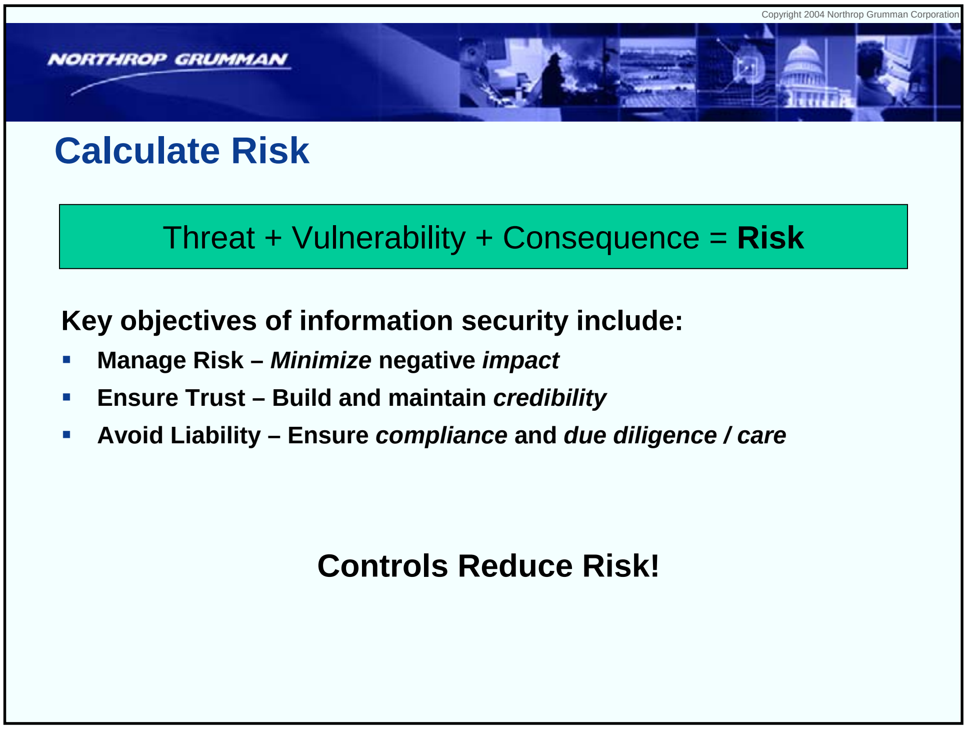
Click here to visit the official WOH site!

Now, A Less Glamorous Example

- You terminate system administrator Bob.
- You don’t disable Bob’s account.
- Bob connects from home and formats your server.
- You have no backups.
- You have no data.



Start With Some Requirements



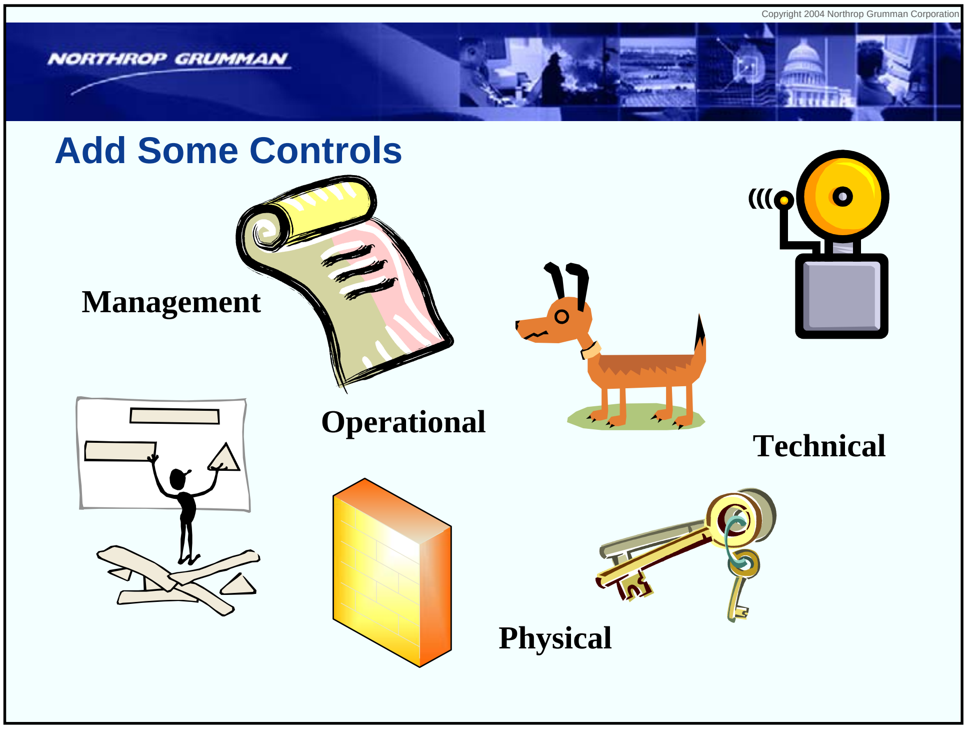
Calculate Risk

Threat + Vulnerability + Consequence = **Risk**

Key objectives of information security include:

- **Manage Risk – *Minimize* negative *impact***
- **Ensure Trust – Build and maintain *credibility***
- **Avoid Liability – Ensure *compliance* and *due diligence / care***

Controls Reduce Risk!



NORTHROP GRUMMAN

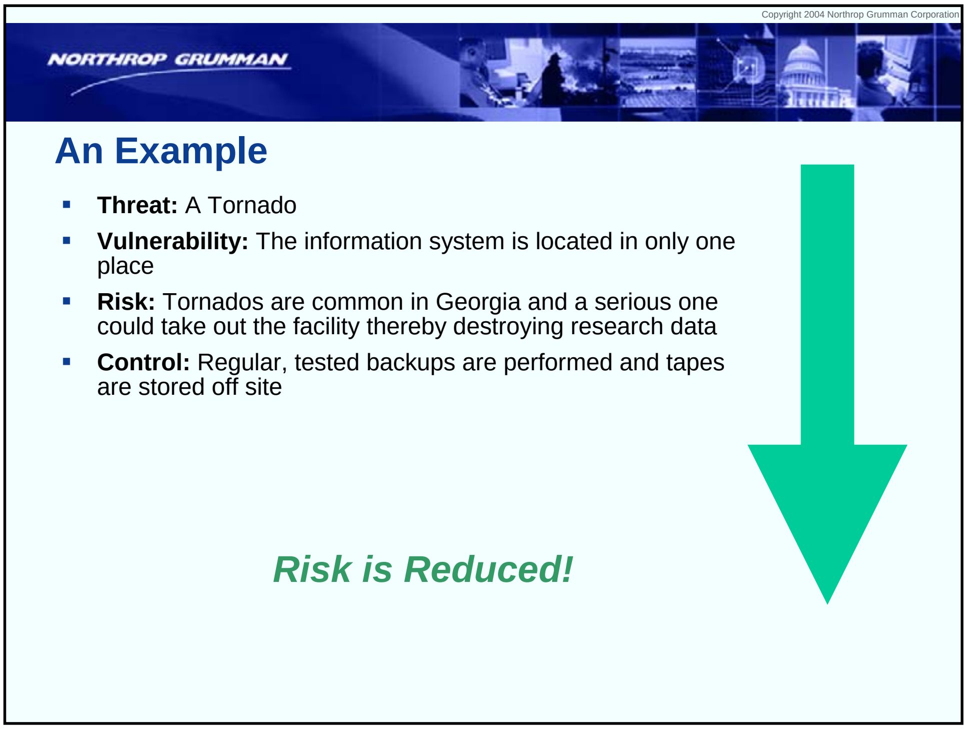
Add Some Controls

Management

Operational

Technical

Physical

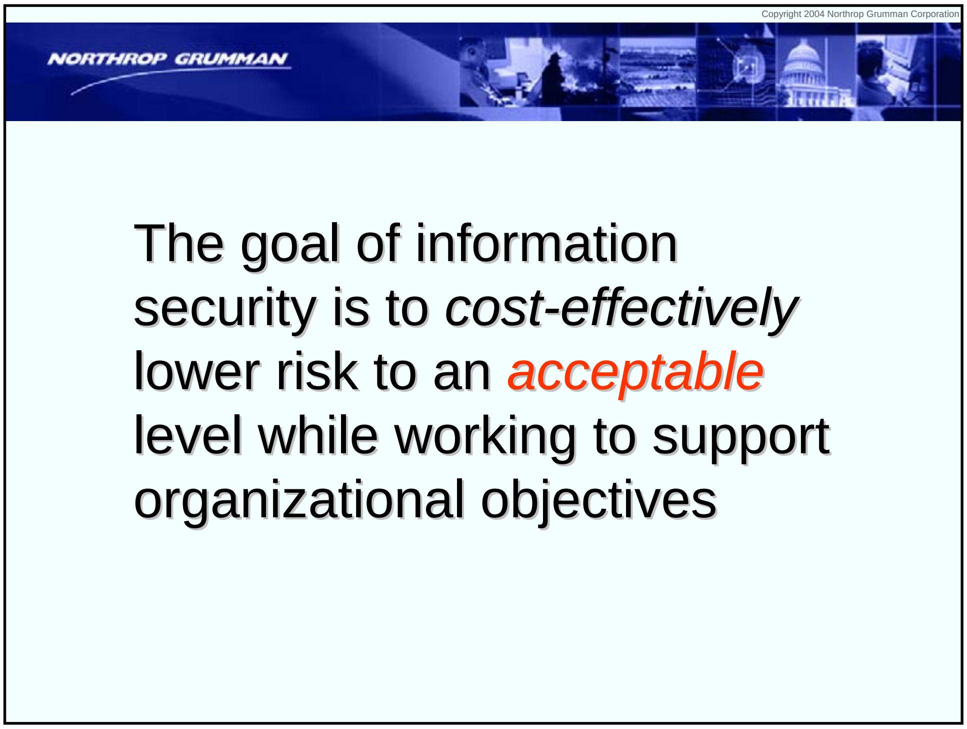


NORTHROP GRUMMAN

An Example

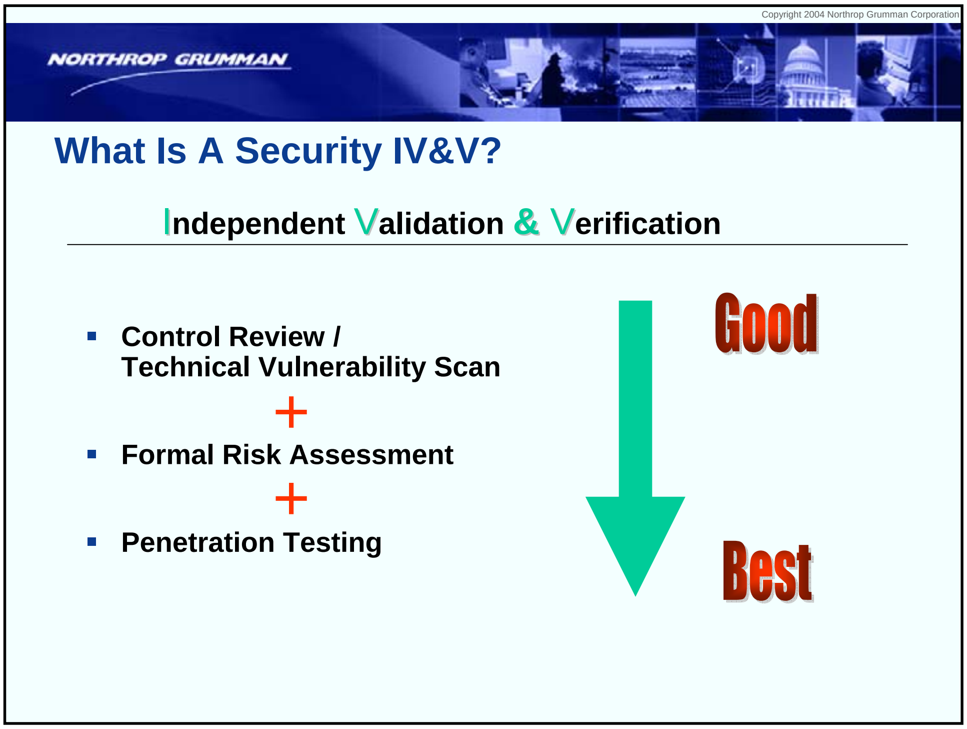
- **Threat:** A Tornado
- **Vulnerability:** The information system is located in only one place
- **Risk:** Tornados are common in Georgia and a serious one could take out the facility thereby destroying research data
- **Control:** Regular, tested backups are performed and tapes are stored off site

Risk is Reduced!



NORTHROP GRUMMAN

The goal of information security is to *cost-effectively* lower risk to an *acceptable* level while working to support organizational objectives



NORTHROP GRUMMAN

What Is A Security IV&V?

Independent Validation & Verification

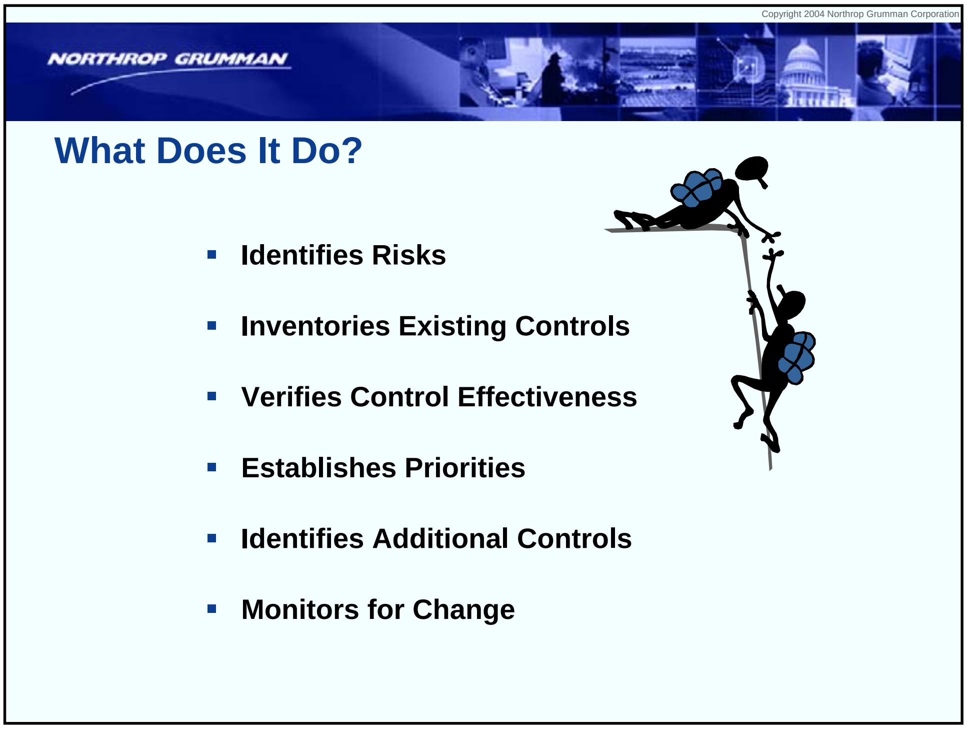
- **Control Review / Technical Vulnerability Scan**

+

- **Formal Risk Assessment**

+

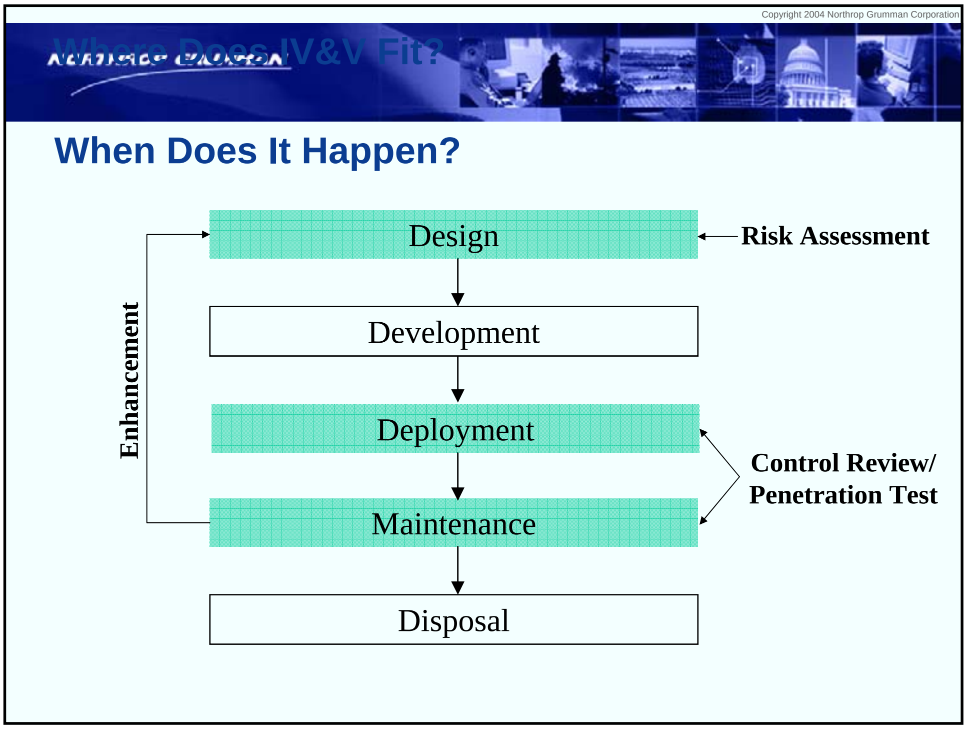
- **Penetration Testing**



NORTHROP GRUMMAN

What Does It Do?

- Identifies Risks
- Inventories Existing Controls
- Verifies Control Effectiveness
- Establishes Priorities
- Identifies Additional Controls
- Monitors for Change



Where Does IV&V Fit?

When Does It Happen?

Design

Development

Deployment

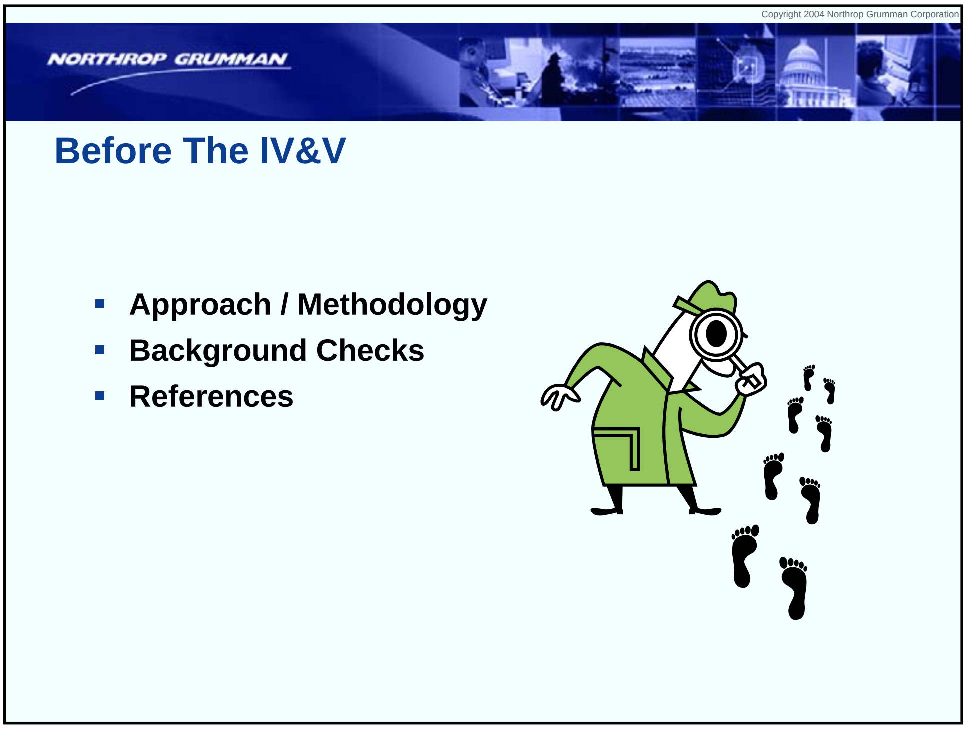
Maintenance

Disposal

Enhancement

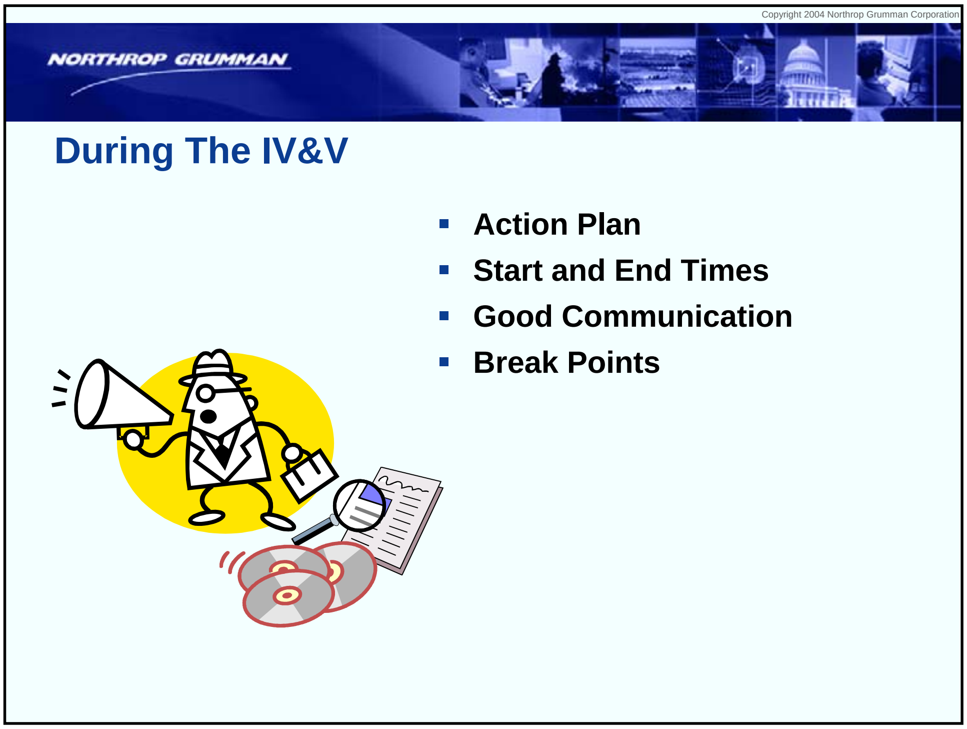
Risk Assessment

Control Review/
Penetration Test



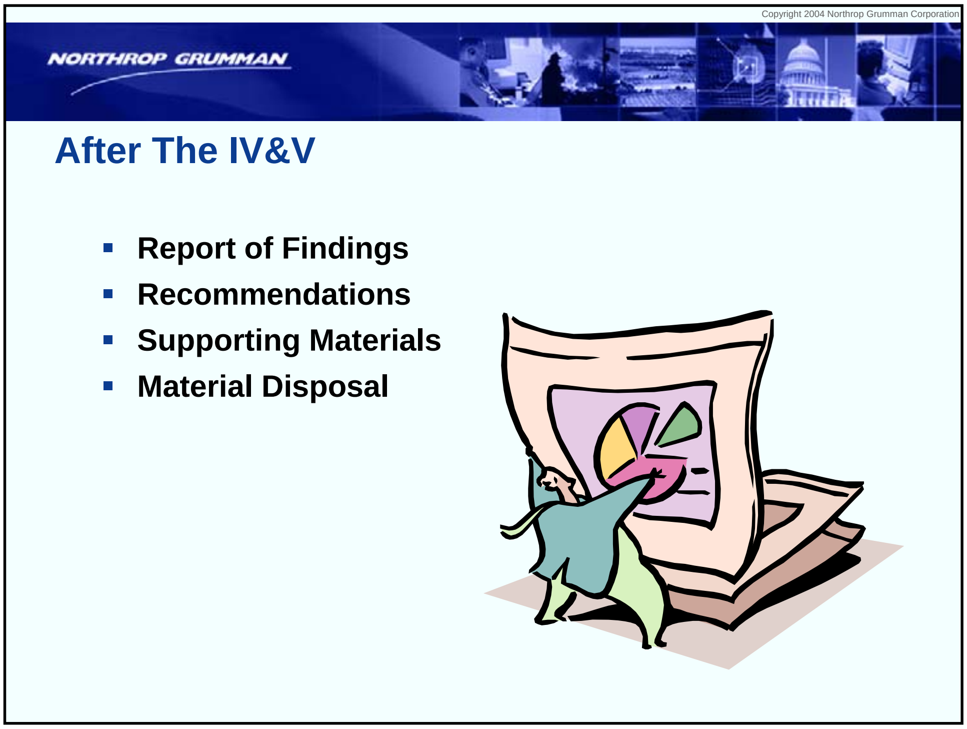
Before The IV&V

- Approach / Methodology
- Background Checks
- References



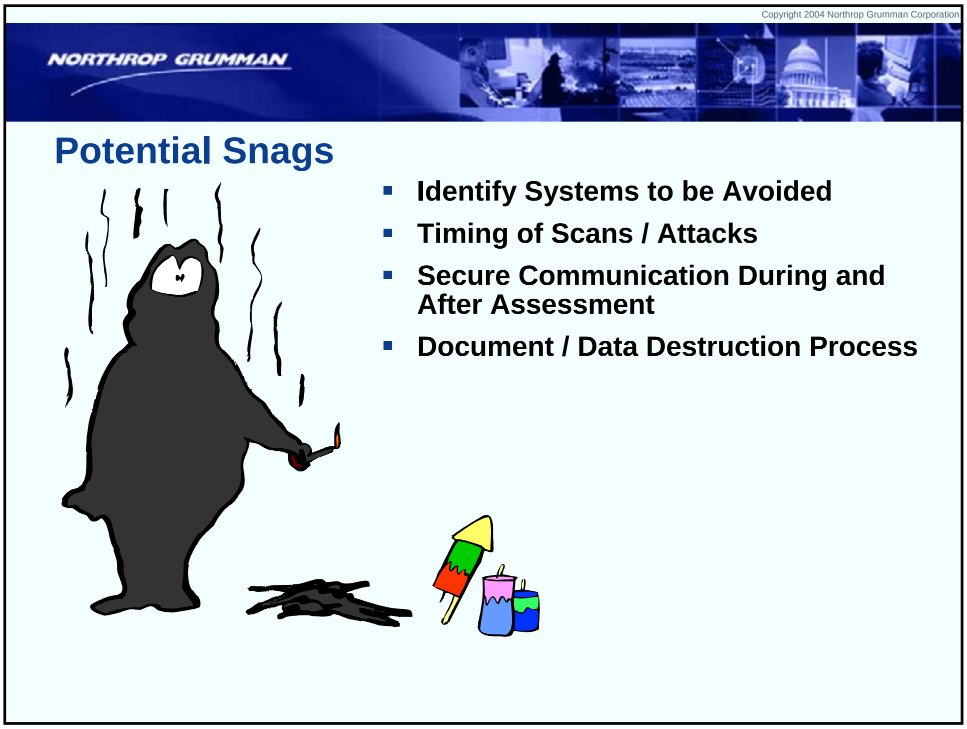
During The IV&V

- Action Plan
- Start and End Times
- Good Communication
- Break Points



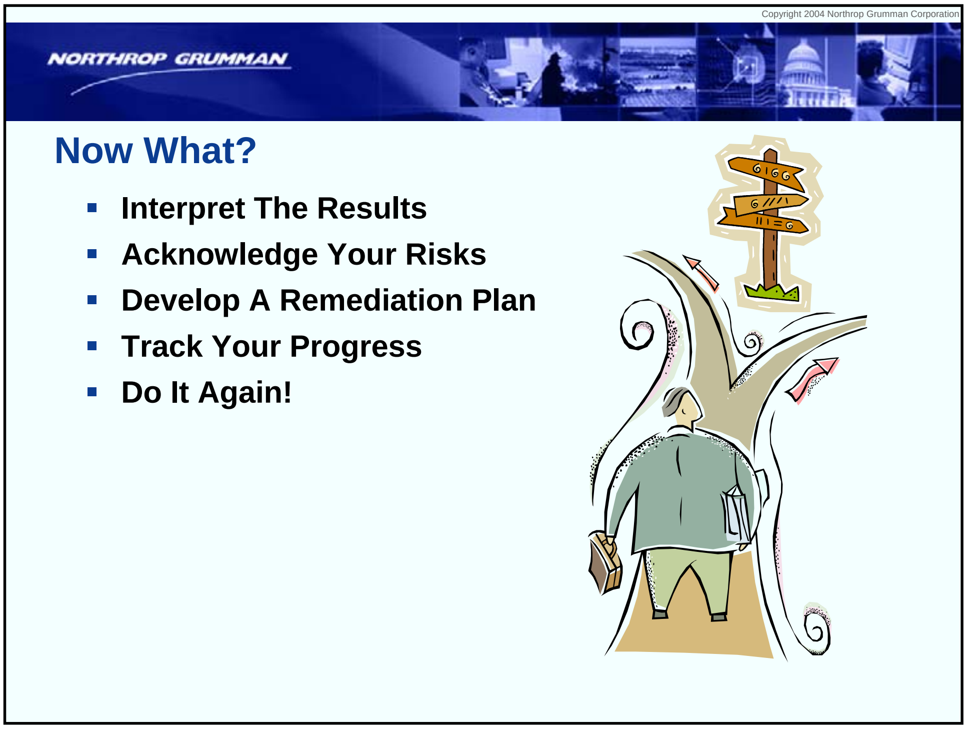
After The IV&V

- Report of Findings
- Recommendations
- Supporting Materials
- Material Disposal



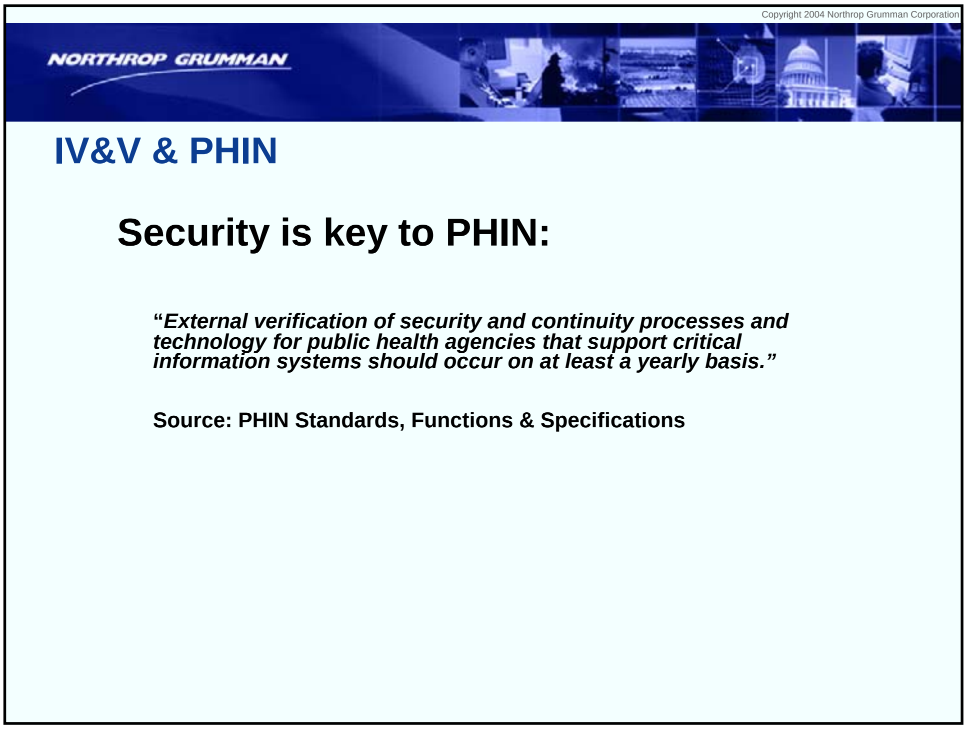
Potential Snags

- Identify Systems to be Avoided
- Timing of Scans / Attacks
- Secure Communication During and After Assessment
- Document / Data Destruction Process



Now What?

- Interpret The Results
- Acknowledge Your Risks
- Develop A Remediation Plan
- Track Your Progress
- Do It Again!

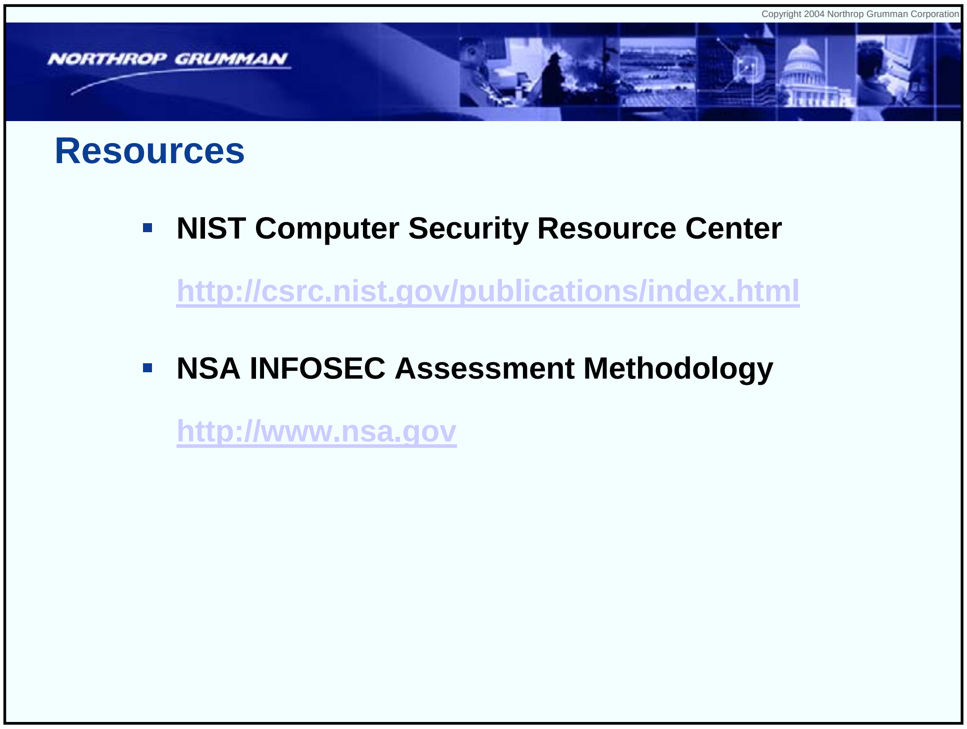


IV&V & PHIN

Security is key to PHIN:

"External verification of security and continuity processes and technology for public health agencies that support critical information systems should occur on at least a yearly basis."

Source: PHIN Standards, Functions & Specifications



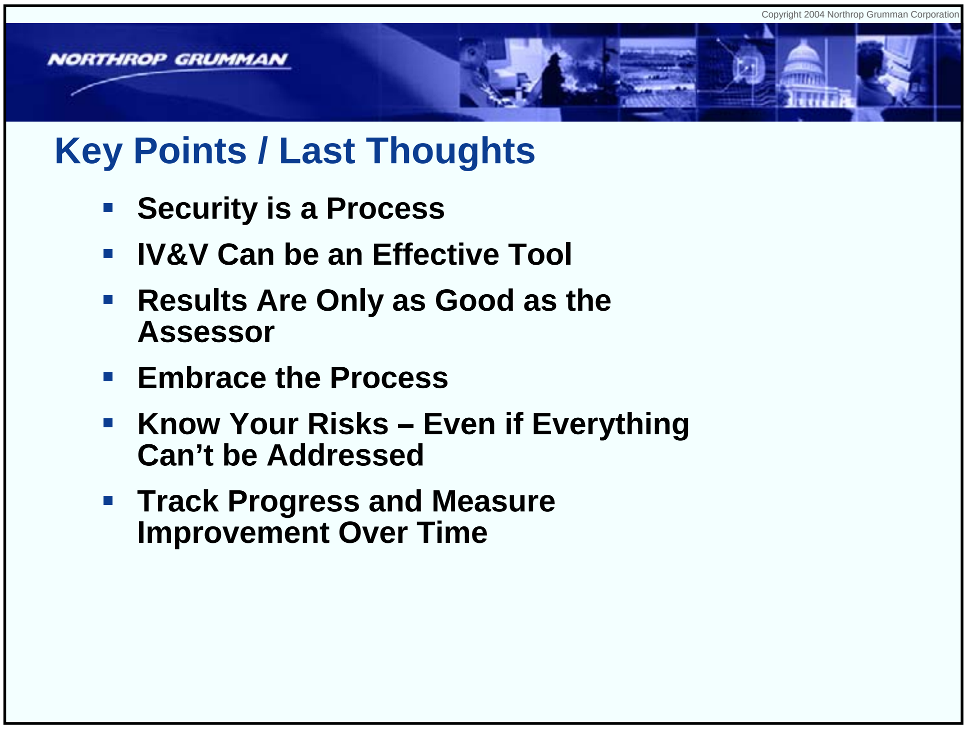
Resources

- NIST Computer Security Resource Center

  http://csrc.nist.gov/publications/index.html

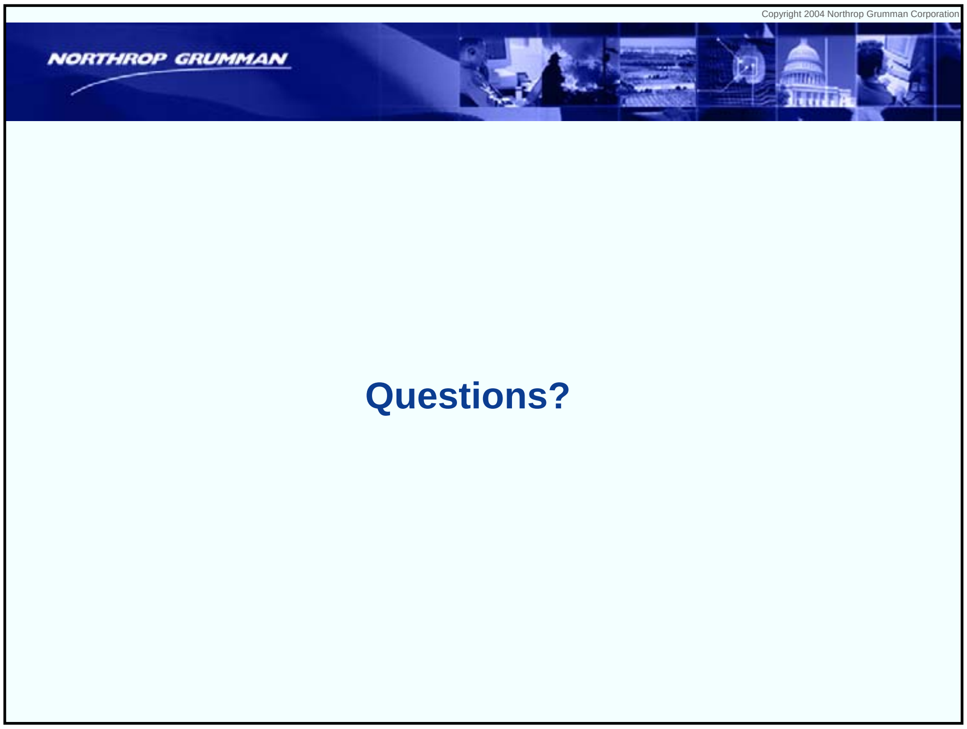
- NSA INFOSEC Assessment Methodology

  http://www.nsa.gov



Key Points / Last Thoughts

- Security is a Process
- IV&V Can be an Effective Tool
- Results Are Only as Good as the Assessor
- Embrace the Process
- Know Your Risks – Even if Everything Can't be Addressed
- Track Progress and Measure Improvement Over Time



NORTHROP GRUMMAN

Questions?